



UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)information associated with Snap Inc. username "loweffortname6" and
"td0815" that is stored at premises owned, maintained, controlled, or
operated by Snap Inc. with company headquarters in Santa Monica, CA

Case No. 25 MJ 122

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Please see Attachment A.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2252A(a)(5)(B)	possession, distribution and receipt of child pornography
18 U.S.C. 2251(a) and (e)	attempted production of child pornography

The application is based on these facts:

Please see Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Nathan Markon, Special Agent - FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 06/25/2025

Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Nathan Markon, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Snapchat account that is stored at premises owned, maintained, controlled, or operated by Snap Inc., a company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Snap Inc. to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account.

2. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since July 2024 and am currently assigned to the Milwaukee Division as a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. My duties include investigating criminal violations relating to child sexual exploitation and child pornography. While employed by the FBI, I have investigated federal criminal violations related to child exploitation and child pornography. I have received training from the FBI specific to investigating child pornography and child exploitation crimes and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media. As a result of my training, experience, and discussions with other law enforcement officers assigned to investigate child pornography and child exploitation, I am familiar with methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing

images and videos depicting minors engaged in sexually explicit conduct. I have also received training and gained experience in interview and interrogation techniques with enhanced training specific to cybercrimes, social media search warrants, residential search warrants, interviews and interrogations of subjects of criminal investigations, electronic device identification and forensic review.

3. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law enforcement officers, who have provided information to me during the course of their official duties and whom I consider truthful and reliable.

4. Based upon the information described below, I submit that probable cause exists to believe that the user of Snapchat accounts in the name of “**loweffortname6**” and “**td0815**” (the SUBJECT ACCOUNT) has committed the crime of attempted production of child pornography, in violation of Title 18, United States Code, Section 2251(a), receipt/distribution of child pornography in violation of Title 18, United States Code, Section 2252(a)(2), and possession of child pornography in violation of Title 18, United States Code, Section 2252(a)(4)(B). I further submit that evidence relating to this crime, more particularly described in Attachment B, can be found in the contents of the SUBJECT ACCOUNT, more particularly described in Attachment A. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. 2711. 18 U.S.C. 2703(a), (b)(1)(A), & (c)(1)(A).

Specifically, the court is “a district court of the United States, that has jurisdiction over the offense being investigated.” 18 U.S.C. 2711(3)(A)(i).

DEFINITIONS

6. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. “Child Pornography” is defined in 18 U.S.C. § 2256 as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. Child pornography is also commonly referred to as Child Sexual Abuse Material, or “CSAM.”

b. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. “An Internet Protocol address” (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series

of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

e. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

f. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

h. “Visual depictions” include undeveloped film and videotape, and data stored on a computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

i. “Website” consists of text pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol.

BACKGROUND ON SNAPCHAT

7. Snapchat is a messaging and image-sharing platform run by Snap Inc. that connects users with their friends, family, and the world through chat, voice, image and video messaging. Snapchat has both a web application and a mobile device (iOS, Android) application, and the service can also be accessed from the website directly at www.snapchat.com.

8. In order to use the services, users need to create an account by selecting a username. Once they’ve made their account, users can create Snaps, Stories, Memories, or Chat.

9. Snaps are photos or videos taken using the Snapchat app’s camera on an individual’s mobile device. Snaps may be shared either directly in a Chat with one or a group of the user’s friends, or shared in a Story (explained below). Snapchatters can save a Snap message by pressing and holding on it to save while viewing or directly after viewing a Snap. After saving a Snap, the Snap will appear in the conversation as Chat Media. (Chat Media is discussed in the Chat section below.) Snap’s servers are designed to automatically delete a shared Snap after it has been opened by all recipients.

10. A user can add Snaps, Memories, or images and video from their device camera roll to their “Story.” In general, users can manage their privacy settings so that their Story may be able to be viewed by all Snapchatters, their friends, or a custom audience. Users can also elect to create other types of Stories, or to submit content to the Snap Map or Spotlight. Snap’s servers are currently designed to automatically delete the content in a user’s Story, by default, 24 hours after it is shared on Snapchat, but the user may delete part or all of the Story earlier or they may, in certain instances, change their settings to have the Story visible longer. Submissions to the Snap Map and Spotlight may be saved for longer periods.

11. Memories is Snapchat’s cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their device’s camera roll in Memories. Content saved in Memories is backed up by Snap and may remain in Memories until deleted by the user. Users may choose to encrypt their content in Memories by saving it in “My Eyes Only,” in which case the content is not accessible to Snap and cannot be decrypted by Snap. Please note that because Memories functions as cloud storage, Snap will not provide Memories files in response to legal process that requests interpersonal communications.

12. A user can send text and send Snaps in Chat. A user may also send Memories, media uploaded from their device’s camera roll, or audio notes (collectively “Chat Media”) to friends within the Snapchat app using the Chat feature. Users can Chat one-on-one or in groups.

13. If a user has device-level location services turned on and has opted into location services on Snapchat, Snap will collect location data from the device at various points during the user’s use of Snapchat. Retention periods for location data may vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

14. Providers like Snap Inc. typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the SUBJECT ACCOUNT.

15. In some cases, Snapchat users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

1. On or about March 20, 2024, an adult female from the United Kingdom submitted an online tip to the FBI National Threat Operations Center (NTOC). The tip claimed THOMAS DONNELLY, hereafter referred to as the Subject, was grooming minors via social media, including Snapchat, and soliciting, distributing, and possessing CSAM. The complainant claimed the Subject formed an emotional relationship with the complainant, who was an adult at the time of their interaction. According to the complainant, the Subject coerced the complainant into

sending explicit photos of herself next to pictures of herself as a minor. The Subject also coerced her into roleplaying wherein the complainant would take the role of a 12-year-old. The complainant listed the Subject's age as 40 years old.

2. The tip also claimed that the Subject coerced her into watching CSAM and that she observed him masturbating to the CSAM. The Subject introduced the complainant to a 14-year-old girl that lives in Wisconsin. The Subject claimed to be in a relationship with the 14-year-old girl. The complainant spoke with the 14-year-old girl multiple times. The Subject sent the complainant CSAM of the 14-year-old girl, as well as other minor females.

3. On or about March 21, 2024, a Special Agent with FBI-Milwaukee interviewed the complainant via telephone. The complainant claimed the Subject lives in the area of New Berlin, Wisconsin. The complainant also provided multiple social media usernames for the Subject, including the Discord username "FrankiePeanuts" and Snapchat username "**loweffortname6**."

4. A Special Agent with FBI-Milwaukee requested a search of CyberTipline Reports from the National Center for Missing and Exploited Children (NCMEC) with the search term "THOMAS DONNELLY" and various social media usernames associated with the Subject. CyberTipline Report 183924709, generated on January 7, 2024 from Discord identifies username ".frankiepeanuts", with associated email "limitlessanonymity@gmail.com", as uploader of one file of Child Pornography.

5. On or about January 31, 2025, FBI Milwaukee received the media file associated with CyberTipline Report 183924709. The file is described:

- a. Image 1 is a horizontally oriented full-color image. The image depicts a naked adult male kneeling on a blue padded surface. The adult male is visible from the chest to knees. A prepubescent female approximately three to five years old is laying on her

back in front of the adult male. Her torso, one leg, and one arm are visible. The adult male is kneeling between the prepubescent female's legs. The prepubescent female is wearing a pink and white shirt that is pulled up to expose her stomach. The adult male is holding his penis with one hand and the prepubescent female's leg with the other. The adult male is pushing his penis down on top of the prepubescent female's vagina, creating partial vaginal penetration with his penis.

6. On or about March 5, 2025, a Court Order signed by United States Magistrate Judge William Duffin was served to Snap Inc. for target identifiers linked to the Subject, including usernames "**loweffortname6**" and "**td0815**". On or about March 10, 2025, Snap Inc. provided returns, including a "friends" list associated with "**loweffortname6**." One user on the Subject's friends list, hereafter known as "User 1", was noted as blocked and deleted within the returns.

7. Through legal process and open-source research User 1 was identified and found to be living in the United States, in the southeastern area of the country. FBI Agents contacted User 1's family, who identified User 1 as a minor, year of birth 2008. An interview was scheduled between User 1 and an FBI Child and Adolescent Forensic Interviewer (CAFI).

8. During that interview on May 6, 2025, User 1 disclosed she met the Subject online on a Discord server in the fall of 2023, when she was 15 years old. User 1 identified the Subject's Discord username, ".frankiepeanuts", as belonging to the Subject. User 1 identified the phone number associated with the "**loweffortname6**" Snapchat account. User 1 stated she had also communicated with the Subject on Snapchat, which requires both users to be "friends" on Snapchat. User 1 also identified the Subject by name based on a driver's license photo shown to her.

9. During the forensic interview, User 1 disclosed that the Subject solicited her for nude pictures. According to User 1, the Subject directed User 1 to undress, then to strike herself

to the point of leaving marks or bruises. The Subject also directed User 1 to choke, cut, and burn herself while video chatting. The Subject took screenshots of User 1 in various states of undress and after conducting self-harm. User 1 told the forensic interviewer that she could hear clapping noises and heavy breathing during these video chats, implying the Subject was masturbating.

10. If User 1 didn't comply with the Subject's directions, the Subject would threaten to harm User 1's friends or other people. In at least one instance, the Subject threatened to go outside his residence and find someone to hurt if User 1 did not remove her clothes during a video chat. The Subject knew some of User 1's online friends and threatened to make them self-harm.

11. According to User 1 the Subject made other requests of User 1 that covered a range of other sexual topics. These topics included asking her to drink her own urine and if he could send her a video depicting bestiality. He referenced wanting to have a child with User 1, and then sexually abuse that child. The Subject referenced wanting to sell nude pictures of User 1.

12. According to User 1, the Subject sent sexually explicit media to User 1, including a 30 second video of the Subject's girlfriend, an adult known to the investigators, conducting oral sex on the Subject.

13. According to User 1, the Subject directed User 1 to communicate with another user via Tumblr, hereafter known as User 2. User 2 is an adult male known to investigators. The Subject told User 1 he wanted her to communicate with User 2 because the Subject wanted User 1 to gain sexual experience. User 2 was geographically close to User 1. In August 2024 User 2 met with User 1 and took her to a hotel late at night, where User 2 sexually abused User 1. User 1 observed User 2 pointing their phone camera at User 1 while User 2 sexually abused User 1.

14. On June 16, 2025, the FBI was made aware of a second NCMEC CyberTipline Report, number 208367814. This report named username “tiredolddad1” as the subject of distributing CSAM (child sexual abuse material) via Discord on March 30, 2025, with the associated email “tiredolddad1@gmail.com”. Legal process was served by Wisconsin Department of Justice to trace the IP address used by the email. The IP Address came back to the Subject’s residence. The file distributed by the Subject is described herein:

- a. The file was a color video approximately 1 minute and 51 seconds long. It depicted a white naked prepubescent female minor being sexually assaulted by a male of undetermined age via vaginal intercourse. From the video angle the female appeared to have no breast development. Based on her body structure, size, and facial features the female appeared to be under 10 years old. The female's body appeared hairless. She had dark eyes, dark eyebrow hair, and dark hair on her head. Her hair appeared short or tucked behind her head as she lay supine with her legs spread and arms raised to shoulder height. The female looked upward, to the side, and toward the male. There was an approximately quarter sized circular birthmark or dark spot near the front of her right shoulder. Both of her knees appeared to have scabs on them. The female spoke in a foreign language at the onset of the video. The language sounded similar to German. During the video she made labored breathing and whining sounds as the male thrust into her. She appeared to be on top of a dark colored couch or bed with black pillows, gray pillows, and a multicolored blanket. From the video angle the male of undetermined age appeared to be white and much larger than the female. The front of his lower torso and tops of his upper legs were visible. He appeared hairless. During a portion of the assault he held the right side of the female's torso. His hand was large enough to reach from her navel to the her back.

15. On June 18, 2025, the FBI executed a search warrant signed by United States Magistrate Judge William E. Duffin at the Subject’s residence in Waukesha County, Eastern District of Wisconsin. During the initial preview of the Subject’s personal computer, at least four images of CSAM were found and are described herein:

- a. Images 1 and 2 are two full color pictures depicting an infant, approximately 1-2 years old. The photos are cropped close to only show the infants face. An adult penis is in close proximity to the infant's open mouth.
- b. Image 3 is a full color picture depicting a female toddler. The picture is cropped close to show only the child's face. An adult penis is in the toddler's mouth, with the child's hand around the penis.
- c. Image 4 depicts a pre-pubescent female, approximately 5-8 years old, laying on her back with legs spread apart. An adult male conducts vaginal intercourse with the pre-pubescent female. Visible in the background is a pillow. Also shown in the image is the text: "Contact me" with a web address.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

16. According to Snap Inc.'s law enforcement guide, the following items are available with a search warrant: Basic subscriber information, current and previous Snapchat usernames, current and previous email addresses associated with the account, and whether verified by user, current and previous phone numbers associated with the account, and whether verified by user, current and previous Snapchat display names, Snapchat account creation date and IP address, IP addresses (and timestamps) relating to various Snapchat account actions, certain information about the user's use of Snapchat services and account settings, logs containing metadata about a user's communications, metadata not related to communications, such as Friends List or device identifier information, logs regarding Memories metadata, location data for a Snapchatter who has enabled location services on their device and opted into location services in the Snapchat app settings, and content specifically saved by the Snapchatter.

17. As explained herein, information stored in connection with a Snap Inc. account may provide crucial evidence of the "who, what, why, when, where and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or

alternatively, to exclude the innocent from further suspicion. In my training and experience, a messaging application user's communication logs, stored electronic communications, and other data retained by Snap Inc., can indicate who has used or controlled the Snapchat account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Snapchat account activity can show how and when the account was accessed or used. For example, as described herein, Snap Inc. logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Snapchat access, use, and events relating to the crime under investigation. Additionally, Snapchat account activity may provide relevant insight into the Snapchat account owner's state of mind as it relates to the offense under investigation. For example, information in Snapchat chats may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

18. Therefore, the computers of Snap Inc. are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Snapchat, such as account access information, transaction information, and other account information.

SEARCH PROCEDURE

19. From my training and experience, I know that Snapchat cannot, on its own, identify individual items of potential evidentiary value within user's account. Accordingly, this search warrant anticipates a multi-step approach for serving the warrant, obtaining responsive information from Snap Inc., and then searching the responsive information to identify potential evidence.

20. Pursuant to the Electronic Communications Privacy Act, in particular 18 U.S.C. 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), I will serve the warrant on Snap Inc. Snap Inc. will, at a later date, disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Attachment B. Once received, the government will search the records and information provided by Snap Inc. to locate items and evidence relating to the crimes under investigation, specifically Title 18 U.S.C. 2252A, including:

- a. Messages discussing child pornography;
- b. Photographs, videos, or images of child pornography
- c. Chats discussing child pornography
- d. Chats between the user and any minor;
- e. Chats between the user and any known or potential victims
- f. Evidence indicating how and when the account was accessed or used, to determine the chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- g. Evidence indicating the account owner's state of mind as it relates to the crime(s) under investigation;
- h. All items tending to show who was in control of the account and who used or owned the device(s) associated with this account including email addresses, images, recovery

emails, cookies data, geolocation data, documents, IP logs, and other communication records; and

- i. All other information or items that constitute fruits, contraband, evidence, or instrumentalities of violations of 18 USC § 2252, those violations involving the Subject Account and occurring since September 1, 2023.

CONCLUSION

23. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Snap Inc., who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Attachment A
Property to be Searched

This warrant applies to information associated with Snap Inc. username “**loweffortname6**” and “**td0815**” that is stored at premises owned, maintained, controlled, or operated by Snap Inc. with company headquarters at 2772 Donald Douglas Loop North, Santa Monica, California.

Attachment B
Particular Things to be Seized

I. Information to be disclosed by Snap Inc.

To the extent that the information associated with the account described in Attachment A is within the possession, custody, or control of Snap Inc., regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Snap Inc., or have been preserved pursuant to a request made, Snap Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A, from September 1, 2023 to the present:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- b. The types of service utilized by the user;
- c. All records or other information stored by an individual using the account, including saved communications, image files or video files;
- d. All records pertaining to communications between Snap Inc. and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. 2252(a)(2), 2251(a), and 2252(a)(4)(B) involving the account described in Attachment A since September 1, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Images of child pornography, as defined in 18 U.S.C. 2256.
- b. Any record or document pertaining to the possession, receipt, and/or distribution of child pornography, as defined in 18 U.S.C. 2256.
- c. Any record or document identifying persons transmitting, through interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256.

- d. Any record or document bearing on the receipt, shipment, orders, requests, trades, purchases or transactions of any kind involving the transmission through interstate commerce, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256.
- e. Any record or document pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the receipt, distribution, trade, or transmission, through interstate commerce, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256.
- f. Any record or document which lists names and addresses of any minor visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256.
- g. Any record or document which shows the offer to transmit through interstate commerce any depictions of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256.
- h. Any and all materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as, "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings. "Child erotica," may also include, in this context, sex aids and/or toys.
- i. Electronically stored communications or messages reflecting computer online chat sessions or e-mail messages with, or about, a minor that are sexually explicit in nature, as defined in 18 U.S.C. § 2256.
- j. The identity of the person(s) who created or used the account listed in Attachment A, including records that help reveal the whereabouts of such person(s).
- k. The identity of the person(s) who communicated with the account listed in Attachment A about matters relating to 18 U.S.C. 2252A(a)(2) and 2252A(a)(5)(B), including records that help reveal their whereabouts.
- l. Chats between the user and any minor.
- m. All other information or items that constitute fruits, contraband, evidence, or instrumentalities of violations of 18 USC § 2252, those violations involving the Subject Account and occurring since September 1, 2023.

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.